

Appl. No. 10/702,540  
Reply to Office Action of March 29, 2007

RECEIVED  
CENTRAL FAX CENTER

MAY 29 2007

REMARKS/ARGUMENTS

Status of the Claims

Claims 1-23 and 34-43 remain in the application.

Claim Amendments

Claim 40 has been amended to recite in part:

"said data content server operable to transmit the plurality of decryption keys in a manner such that the data content download controller has simultaneous possession of at most a subset of the plurality of decryption keys at any time."

Interview Summary

We thank the Examiner for a telephone interview on May 23, 2007. The interview is briefly summarized below.

The purpose of the interview was to discuss the primary reference cited in the current Office Action, namely U.S. Patent Application Publication No. 2002/0170053 A1 (Peterka et al.). In particular, it is Applicant's opinion that Peterka et al. fails to teach or fairly suggest one of the key limitations of the independent claims, namely

"delivering to the customer processing platform a plurality of decryption keys corresponding to the plurality of encryption keys, wherein the decryption keys are delivered in a manner such that the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time."

In the current Office Action, the Examiner has pointed to Figure 7 and paragraphs [0080], [0082], [0093] and [0102] of Peterka et al. in support of the allegation that Peterka et al.

Appl. No. 10/702,540

Reply to Office Action of March 29, 2007

discloses the above limitation. However, in the interview, Applicant pointed out that these portions of Peterka et al. fail to disclose the above limitation, and instead merely teach that Program Service Keys (PSKs) or Content Keys (CKs) are made sequentially available to the customer, and in some cases a current key for a current encrypted section and a next key for the next encrypted section are made available at the same time to avoid congestion at a key server. In response, the Examiner stated that we were incorrect in merely analyzing these portions of Peterka et al. alone, and must instead consider Peterka et al. as a whole. We contended that Peterka et al. as a whole fails to teach or fairly suggest the above limitation, and requested that the Examiner identify a specific portion of Peterka et al. that discloses the above limitation. The Examiner was unable to identify a specific portion of Peterka et al. that does so, and instead insisted that the delivery of a current key and a next key according to Peterka et al. is equivalent to the delivering the plurality of decryption keys to the customer processing platform in a manner such that the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time.

Applicant pointed out that merely making a current key and a next key available simultaneously certainly does not prevent the customer processing platform from having simultaneous possession of the entire plurality of decryption keys. Therefore, according to the teachings of Peterka et al., once the client has received all of the decryption keys, the client has simultaneous possession of the entire plurality of decryption keys, which would allow the client to decrypt the encrypted content at will. Accordingly, Peterka et al. offers no protection from piracy or duplication of the decrypted content.

In an effort to overcome our contrary views of the cited reference, the Examiner suggested that the independent claims could be amended to include an explicit description of the key deletion/destruction process. The Examiner indicated that if a limitation were included in the independent claims that recited that a current decryption key was deleted prior to receiving a next decryption key, such independent claim would likely distinguish over the currently cited references. However, this additional limitation is considered to be unnecessarily limiting, given our position that Peterka et al. fails to disclose any mechanism by which a client is prevented

Appl. No. 10/702,540  
Reply to Office Action of March 29, 2007

from having simultaneous possession of an entire set of decryption keys. Furthermore, such a limitation is already present in claims 2, 3, 4, 5, 6, 16, 34 and 39.

### **35 U.S.C § 102 Claim Rejections**

In paragraph 3 of the Office Action, the Examiner rejects claims 1, 7-13, 15, 35-37, 38 and 40-42 under 35 U.S.C. § 102(e) as being anticipated by Peterka et al. (U.S. Patent Application Publication No. 2002/0170053 A1).

Before setting forth a discussion of the prior art applied in the Office Action, it is respectfully submitted that controlling case law has frequently addressed rejections under 35 U.S.C. § 102. "For a prior art reference to anticipate in terms of 35 U.S.C. Section 102, every element of the claimed invention must be identically shown in a single reference." *Diversitech Corp. v. Century Steps, Inc.*, 850 F.2d 675, 677, 7 U.S.P.Q.2d 1315, 1317 (Fed. Cir. 1988; emphasis added). If any claim, element, or step is absent from the reference that is being relied upon, there is no anticipation. *Kloster Speedsteel AB v. Crucible, Inc.*, 793 F.2d 1565, 230 U.S.P.Q. 81 (Fed. Cir. 1986; emphasis added). The following analysis of the present rejections is respectfully offered with guidance from the foregoing controlling case law decisions.

Applicant respectfully submits that Peterka et al. fails to teach or fairly suggest key limitations of independent claims, and therefore Peterka et al. cannot be found to anticipate the present invention given the rulings in *Diversitech Corp. v. Century Steps, Inc.* and *Kloster Speedsteel AB v. Crucible, Inc.* Specifically, Applicant respectfully submits that Peterka et al. fails to teach or even suggest

"delivering to the customer processing platform a plurality of decryption keys corresponding to the plurality of encryption keys, wherein the decryption keys are delivered in a manner such that the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time.", as recited in independent claim 1, and as similarly recited in independent claims 35, 37, 38 and 40.

Appl. No. 10/702,540  
Reply to Office Action of March 29, 2007

Peterka et al. describes a method for distributing encrypted data content which uses a hierarchy of encryption keys to provide for flexible billing options. Specifically, Peterka et al. describes a Pay-By-Time (PBT) billing option (See [0048]) in which a program is segmented into a plurality of program segments. The actual data of each respective program segment is then encrypted with at least one respective content key (CK). The respective content keys are then each encrypted with a respective program segment key (PSK). When a consumer wishes to join a multicast of the program, the consumer contacts an Origin Content Server (OCS) to begin receiving PSKs. The PSKs are distributed to the consumer in a multicast in which the PSKs are encrypted with the consumer's unique key (UK). In order to actually view a program segment, the consumer must first decrypt the PSK corresponding to that program segment with the consumer's UK, then use that decrypted PSK to decrypt the CK corresponding to that program segment and then finally decrypt that program segment with the decrypted CK. In the Pay-By-Time billing method, the consumer must continue to request each new PSK in order to continue viewing the program, i.e. to continue decrypting program segments. Peterka also teaches that the content key for a future program segment may be encrypted with not only the PSK corresponding to the future program segment, but also with an old PSK of an old program segment. "Thus, if a user has not yet received a new program segment key, the content key can be obtained by utilizing the old program segment key." (see [0109] and Figure 9). Furthermore, Peterka et al. teaches that the content keys are maintained by the consumers, for possible use in later decryption. For example, Peterka describes a signalling method in which "a predetermined bit can be used to indicate if an **old or current content key should be used as opposed to a new content key** which has recently been distributed to the client." (see [0119]; emphasis added)

On pages 11 of the Office Action, the Examiner has alleged, in support of his rejection of claims 1, 15 and 38, that Figure 7 and paragraphs [0080], [0082], [0093] and [0102] of Peterka et al. disclose the following feature of claims 1, 15 and 38:

"delivering to the customer processing platform a plurality of decryption keys corresponding to the plurality of encryption keys, wherein the decryption keys are delivered in a manner such that the customer processing platform has simultaneous

Appl. No. 10/702,540  
Reply to Office Action of March 29, 2007

possession of at most a subset of the plurality of decryption keys at any time."

The Examiner has further stated that Peterka et al. teaches that the "client has possession of program segment key and the next key ... as well as content keys 0, 1, 2, 3, 4, ...". However, it is respectfully submitted that Peterka et al. does not disclose the above feature, and that the portions of Peterka et al. that the Examiner asserts teach that the "client has possession of program segment key and the next key" merely teach that a current program segment key and a subsequent program segment key are made available to the client at any one given time. It is respectfully submitted that simply making available only a subset of the PSKs at any given time does not guarantee that the client only has simultaneous possession of at most a subset of the PSKs. Accordingly, there is no suggestion in Peterka et al. that if all of the decryption keys have been delivered to the client, the client only has simultaneous possession of at most a subset of the plurality of decryption keys. In fact, the Examiner's own admission that the "client has possession of program segment key and the next key ... as well as the content keys 0, 1, 2, 3, 4, ..." (emphasis added), illustrates that according to Peterka et al., the client has simultaneous possession of all of the content keys once all of the content keys have been received by the client. In contrast, embodiments of the present invention prevent a client from simultaneously having all of the encrypted content and all of the decryption keys necessary to decrypt the encrypted content. Peterka et al. does not provide this same anti-piracy functionality.

In view of the foregoing, it is respectfully submitted that Peterka et al. fails to teach all of the limitations of independent claims 1 and 38.

With regard to the Examiner's novelty rejection of independent claims 35, 37 and 40, it is respectfully submitted that independent claims 35, 37 and 40 share the same distinguishing limitation of claims 1 and 38 identified above, and therefore distinguish over the teachings of Peterka et al. for at least the same reasons.

By virtue of their claim dependencies on one of the independent claims, it is respectfully submitted that dependent claims 7-13, 15, 36, 41 and 42 distinguish over Peterka et al. for at least

Appl. No. 10/702,540  
Reply to Office Action of March 29, 2007

the same reasons.

It is further submitted that dependent claim 7 recites an additional distinguishing feature over Peterka et al. Specifically, it is respectfully submitted that Peterka et al. fails to teach the following limitation of claim 7:

"billing a customer for delivery of the encrypted sections, and then billing the customer each time the data content is used at the customer processing platform".

The Examiner has pointed to Figures 8 and 9 of Peterka et al. in support of the rejection of claim 7. Figures 8 and 9 of Peterka et al. illustrate encrypted data content distribution methods that include: receiving a request for a cryptographic key from a client; logging the request for the key; logging a segment of the program content for which the key can be used; distributing one or more decryption keys; **distributing program content for decryption by the client utilizing the key; and billing the client based upon log entry(ies)**. Therefore, according to Figures 8 and 9 of Peterka et al., and Peterka et al. as a whole, a client must request the cryptographic key **and download the program content again** each time the client wishes to use the data content. According to the teachings of Peterka et al., the client is only billed once the client has re-downloaded the key and the program content, which is completely different than "billing a customer for delivery of the encrypted sections, and then billing the customer each time the data content is used at the customer processing platform", as recited in claim 7.

In view of the fact that Peterka et al. fails to teach a key limitation of the claims, and also fails to identically show every element of the claimed invention, as is required to find that a prior art reference anticipates under 35 U.S.C. § 102, given the rulings in *Kloster Speedsteel AB v. Crucible, Inc.* and *Diversitech Corp. v. Century Steps, Inc.* respectively, the Examiner is respectfully requested to withdraw the 35 U.S.C. 102(e) rejection of claims 1, 7-13, 15, 35-37, 38 and 40-42.

### 35 U.S.C § 103 Claim Rejections

Appl. No. 10/702,540  
Reply to Office Action of March 29, 2007

In paragraph 4 of the Office Action, the Examiner has rejected claims 2-6, 16-19, 21-23 and 39 under 35 U.S.C. § 103(a) as being unpatentable over Peterka et al. in view of Stirling et al. (U.S. Patent Application Publication No. 2003/0223583 A1).

To begin, Applicant respectfully submits that a first criterion required to establish a case of *prima facie* obviousness has not been satisfied. That is, the prior art references do not teach all of the claimed features.

The Examiner has pointed to paragraph [0080] of Stirling et al. in support of the rejection of claims 2-6 under 35 U.S.C. § 103(a). Paragraph [0080] of Stirling et al. recites a first layer of security in a secure data content delivery system, in which a key management and distribution system is based on constructive key management. An architecture where the key is constructed from multiple components, tokens, keys and hardware. Paragraph [0080] of Stirling et al. refers to one such exemplary product available from TECSEC called Constructive Key Management (CKM) Software. Paragraph [0080] of Stirling et al. is reproduced below.

[0080] The first layer can utilize a key management and distribution system based on constructive key management, an architecture where the key is constructed from multiple components, token, keys, hardware. One suitable exemplary product is Constructive Key Management (CKM) software by TECSEC. The CKM server software is installed at the NOC and at the exhibitor's play out servers. **The CKM software allows the NOC to create authorization tokens for distribution to digital production facilities and intended exhibitor systems. Once the tokens are received at the clients, authorized users (digital production facilities and exhibitors play out servers) can encrypt or decrypt the digital content. The clients CKM software agents will construct (create) a key when needed for encryption or decryption and destroy the key when no longer needed by the encryption/decryption engine.**(emphasis added)

The Examiner appears to be relying on the statement that "[t]he client CKM software agents will

Appl. No. 10/702,540

Reply to Office Action of March 29, 2007

construct (create) a key when needed for encryption or decryption and destroy the key when no longer needed by the encryption/decryption engine" to support the assertion that Stirling et al. teaches destroying a decryption key when it is no longer needed. However, the CKM software at the server side (Network Operation Center) creates authorization tokens for distribution to digital production facilities and intended exhibitor systems. The tokens allow content to be encrypted and decrypted at client sites. The client CKM software then constructs a key when needed. The client CKM software destroys the key it created, but does not destroy a key that it received from the server, nor does it destroy the authorization token. This is quite different from the present invention, in which client software destroys the key that it receives from the server.

Applicant submits that the Examiner has applied hindsight analysis in rejecting claim 2. Both Peterka et al. and Stirling et al. fail to teach or fairly suggest encrypting a plurality of sections of data content with a corresponding plurality of encryption keys and distributing decryption keys corresponding to the encryption keys to the processing platform of a consumer in a manner such that the consumer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys, as recited in independent claim 1. Dependent claim 2 depends on independent claim 1 and recites in part that a first decryption key is destroyed after a second decryption key is received, which means that the consumer processing platform has simultaneous possession of at most a subset, in this case two, of the plurality of decryption keys. Applicant submits that the Examiner is incorrect in equating the destroying of a decryption key when it is no longer needed by the decryption engine, as taught by Stirling et al., with the destroying of a first decryption key at a customer processing platform after receiving a second decryption key, as recited in claim 2. There is no suggestion in Peterka et al. that any of the decryption content keys (CK) or program segment keys (PSK) are destroyed, let alone that any key is destroyed after a subsequent key is received. The suggestion in Stirling et al. that a decryption key is destroyed after a decryption engine is finished with it, is not sufficient to allow one skilled in the art to arrive at the subject matter of claim 2, namely that a first decryption key is destroyed after a second decryption key is received.

With regard to the Examiner's rejection of claims 3 to 6, the Examiner has relied upon the same

Appl. No. 10/702,540

Reply to Office Action of March 29, 2007

paragraph in Stirling et al., namely paragraph [0080], in rejecting claims 3 to 6 as was relied upon in the rejection of claim 2. Each of the arguments presented in response to the Examiner's rejection of claim 2 are equally applicable to the Examiner's rejection of claims 3 to 6. Applicant submits that claims 3 to 6 distinguish over the teachings of Peterka et al. and Stirling et al. alone and in combination for at least the same reasons as claim 2.

With regard to the Examiner's rejection of claims 16 and 21, the Examiner has relied upon the same portion of Stirling et al., namely paragraph [0080], in support of the rejection of claims 16 and 21 as was relied upon in the rejection of claims 2 to 6. Applicant submits that the arguments presented above with regard to the rejection of claim 2 are also applicable to the rejection of claims 16 and 21. Furthermore, paragraph [0080] of Stirling et al. merely recites that a decryption key may be created when necessary and **destroyed when no longer needed by the decryption engine**. This recitation by Stirling et al. does not recite "destroying the decryption key after completing playback of the encrypted section" (emphasis added), as recited in claims 16 and 21. As described above, Peterka et al. is entirely silent with regard to the destroying of encryption keys after decryption and therefore a combination of Peterka et al. and Stirling et al. would not allow one skilled in the art to arrive at the present invention.

Applicant submits that a *prima facie* case of obviousness cannot be made against claims 16 and 21, as the cited references fail to teach all of the claimed limitations of claims 16 and 21.

With regard to the rejection of claim 17, the Examiner has once again relied on paragraph [0080] of Stirling et al. in the rejection of claim 17. As described above, paragraph [0080] of Stirling et al. relates to the creation of a **decryption key** when necessary and the destroying of the **decryption key** when no longer needed by the decryption engine. Applicant submits that paragraph [0080] of Stirling et al., and Stirling et al. as a whole, does not teach or fairly suggest "destroying **decrypted data content** at the customer processing platform **after completing playback of the encrypted section**" (emphasis added), as recited in claim 17. It is respectfully requested that the Examiner identify a specific portion of Stirling et al. that discloses "destroying **decrypted data content**", as it is respectfully submitted that Stirling et al. merely discloses

Appl. No. 10/702,540  
Reply to Office Action of March 29, 2007

destroying a constructed **decryption key**.

Applicant submits that a *prima facie* case of obviousness cannot be made against claim 17, as the cited references fail to teach all of the claimed limitations of claim 17.

With regard to the rejection of claims 18 and 19, Applicant submits that claims 18 and 19 depend on claim 16 and therefore distinguish over the teachings of Peterka et al. and Stirling et al., alone or in combination, for at least the same reasons as claim 16, as provided above.

With regard to the rejection of claim 22, similar to the rejection of claims 10, 11 and 12, the Examiner has mistakenly relied upon the recitation in Peterka et al. that a encryption key, i.e. a content key (CK), may be encrypted with a key higher in the key hierarchy, i.e. a unique key (UK), for the purposes of multicast transmission, in rejecting claim 22. Claim 22 recites that "each encryption key comprises a respective customer processing platform-specific key which is determined based on an IP address of the customer processing platform". Applicant submits that encrypting a content key for the purposes of multicast transmission is completely different than encrypting the plurality of sections of data content with a plurality of customer processing platform-specific keys which are determined based on an IP address of the customer processing platform.

According to the teachings of Peterka et al., the encrypted content keys are decrypted with the higher level key, i.e. the unique key (UK), and the content keys are then used to decrypt the corresponding program segments. Once the content key is decrypted with the higher level key, it is completely untraceable, as any customer specific information has been stripped during the decryption of the content key. In contrast, the method according to claim 22 provides for traceability of the decryption key and the encrypted data content, because the sections of data content are encrypted with customer processing platform-specific keys.

Applicant submits that a *prima facie* case of obviousness cannot be made against claim 22, as the cited references fail to teach all of the claimed limitations of claim 22.

Appl. No. 10/702,540  
Reply to Office Action of March 29, 2007

With regard to the rejection of claim 23, Applicant submits that claim 23 depends on claim 16 and therefore distinguish over the teachings of Peterka et al. and Stirling et al., alone or in combination, for at least the same reasons as claim 16, as provided above.

With regard to the rejection of claim 39, similar to the Examiner's rejection of claims 16 and 21, Applicant submits that the arguments presented above with regard to the rejection of claim 2 are also applicable to the rejection of claim 39. Furthermore, the Examiner has once again relied on paragraph [0080] of Stirling et al., which as described above merely recites that a decryption key may be created when necessary and **destroyed when no longer needed by the decryption engine**. This recitation by Stirling et al. does not recite "means for destroying the decryption key, **after completing playback of the encrypted section**" (emphasis added), as recited in claim 39. As described above, Peterka et al. is entirely silent with regard to the destroying of encryption keys after decryption and therefore a combination of Peterka et al. and Stirling et al. would not allow one skilled in the art to arrive at the present invention.

Applicant submits that a *prima facie* case of obviousness cannot be made against claim 39, as the cited references fail to teach all of the claimed limitations of claim 39.

In view of the foregoing, Applicant respectfully submits that a *prima facie* case of obviousness cannot be established against claims 2-6, 16-19, 21-23 and 39, since one or more key limitations of each of the claims is missing from both of the cited references. Applicant respectfully submits that claims 2-13, 16-19, 21-23, and 39 are patentable over Peterka et al. and Stirling et al. since a case of *prima facie* obviousness cannot be established.

In Paragraph 5 on page 23 of the Office Action, the Examiner has rejected claims 14 and 33 under 35 U.S.C. § 103(a) as being unpatentable over Peterka et al. in view of Ginter et al. (U.S. Patent Application Publication No. 2006/0218651 A1).

To begin, Applicant respectfully submits that a first criterion required to establish a case of *prima*

Appl. No. 10/702,540  
Reply to Office Action of March 29, 2007

*facie* obviousness has not been satisfied. That is, the prior art references do not teach all of the claimed features.

With regard to the rejection of claim 14, Applicant submits that claim 14 depends on claim 1 and therefore distinguishes over the teachings of Peterka et al. for at least the same reasons as claim 1, namely that Peterka et al. fails to teach or fairly suggest that decryption keys are delivered "in a manner such that the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption at any time".

Applicant submits that a *prima facie* case of obviousness cannot be made against claim 14, as the cited references fail to teach all of the claimed limitations of claim 14.

In paragraph 5 on page 24 of the Office Action, the Examiner has rejected claims 20 and 43 under 35 U.S.C. § 103(a) as being unpatentable over Peterka et al. in view of Stirling et al. and further in view of Ginter et al..

To begin, Applicant respectfully submits that a first criterion required to establish a case of *prima facie* obviousness has not been satisfied. That is, the prior art references do not teach all of the claimed features.

Claims 20 and 43 depend on claims 16 and 40 respectively. In view of the arguments presented above regarding the Examiner's rejection of claims 16 and 40, Applicant submits that Peterka et al. and Stirling et al. fail to teach or fairly suggest key limitations of claims 16 and 40 and hence of claims 20 and 43. Applicant submits that Ginter et al. similarly fails to teach or fairly suggest these key limitations and therefore claims 20 and 43 distinguish over the teachings of Peterka et al., Stirling et al. and Ginter et al. both alone and in combination.

In paragraph 6 of the Office Action, the Examiner has rejected claim 34 under 35 U.S.C. § 103(a) as being unpatentable over Peterka et al. in view of Negawa (U.S. Patent Application Publication No. 2003/0046539 A1).

Appl. No. 10/702,540  
Reply to Office Action of March 29, 2007

To begin, Applicant respectfully submits that a first criterion required to establish a case of *prima facie* obviousness has not been satisfied. That is, the prior art references do not teach all of the claimed features.

The Examiner has pointed to paragraph [0078] of Negawa in support of the rejection of claim 34, alleging that this paragraph teaches "a method of causing a key for a preceding portion of the encrypted data to be deleted from the customer data content processing device", as recited in claim 34. Applicant submits that Negawa recites "a multicast communication system having a multicast server and a plurality of clients belonging to a multicast group. The multicast server **transmits data encrypted by using a first encryption key** to the clients by multicasting, and **transmits the results of encrypting the first encryption key by using a second encryption key** by unicasting to a client subscribed to a data distribution service, among the plurality of clients. The client subscribed to the data distribution service receives the encrypted data and the result. **The client decrypts the result to obtain the first encryption key and decrypts the encrypted data using the first encryption key**" (see Abstract; emphasis added). According to the teachings of Negawa, a client device plugs into a distribution data receiving device (see Figure 4) in order to receive encrypted data content and decryption keys from a content server (see Figure 2). The distribution data receiving device includes a key decryption key holding unit 34 that holds a key decryption key  $K_m$ . Key decryption key  $K_m$  is the "second encryption key" that is used to encrypt the "first encryption key", which is called the group decryption key  $K_{gr}$ . "Key decryption key  $K_m$  is preferably stored (formed) in key decryption key holding unit 34 in the form of a hardware circuit (for example an IC chip) to ensure that key decryption key  $K_m$  cannot easily be read by a third party" (see [0058]).

Paragraph [0078] of Negawa recites that "[w]hen control unit 30 receives a withdrawal request from client 3c, it deletes (or destroys) the key decryption key  $K_m(C)$  held in key decryption key holding unit 34 and deletes (or destroys) the group session key  $K_{gr}$  held in key decryption unit 33". In other words, when the client 3c no longer wishes to decrypt further data content, i.e. the client 3c issues a withdrawal request, the control unit 30 destroys or deletes the key decryption

Appl. No. 10/702,540

Reply to Office Action of March 29, 2007

key Km(C) and the group session key Kgr. This is completely different than "for each subsequent portion of the encrypted data: transmitting to the customer data content processing device a different key to decrypt the subsequent portion of the encrypted data; and causing a key for a preceding portion of the encrypted data to be deleted from the customer data content processing device", as recited in claim 34. For example, according to Negawa, the key decryption key Km is needed to decrypt the unicast message containing the session key Kgr. If the key decryption key Km is deleted or destroyed then there would be no point in "transmitting to the customer data content processing device a different key to decrypt the subsequent portion of the encrypted data" as the customer data content processing device would be unable to decrypt the "different key" in order to decrypt the "subsequent portion of the encrypted data".

It should be noted that Negawa teaches that a higher level decryption key, namely the key decryption key Km, is destroyed or deleted, thus preventing the decryption of a further lower level decryption key such as the session key Kgr. Accordingly, not only does Negawa fail to teach or fairly suggest the particular feature that the Examiner alleges, but modifying the method of Peterka et al. by incorporating the method of higher level key deletion according to Negawa would render Peterka et al. unsuitable for its intended purpose. Peterka et al. teaches a hierarchy of encryption keys for multicast distribution of encrypted digital content. According to Peterka et al. a content key (CK) is used to encrypt a section of digital content and the content key (CK) is then encrypted with one or more keys that are higher in the key hierarchy than the encryption key. For example, the content key (CK) may be encrypted with a program segment key (PSK) that is in turn encrypted with a unique key (UK) that is unique to a consumer and allows the consumer to decrypt the PSK and hence the CK. If the unique key (UK) of the consumer's processing platform is deleted, the consumer would be only unable to decrypt the PSK and hence the CK for subsequent content segments, but would also cause the consumer to be unable to request subsequent PSKs, due to the fact that the UK is required to "initiate the key request message exchange with a particular caching server" (see [0097] of Peterka et al.). If the UK is deleted, the customer would have to re-register with the content provider in order to receive a new UK, which would render the teachings of Peterka et al. unsuitable for its intended purpose.

Appl. No. 10/702,540  
Reply to Office Action of March 29, 2007

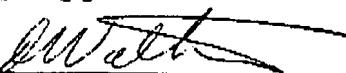
Applicant submits that a *prima facie* case of obviousness cannot be made against claim 34, as the cited references fail to teach all of the claimed limitations of claim 34 and the incorporation of the subject matter of Negawa would render the operation of Peterka et al. unsuitable for its intended purpose.

In view of the forgoing, early favorable consideration of this application is earnestly solicited. In the event that the Examiner has concerns regarding the present response the Examiner is encouraged to contact the undersigned at the telephone number listed below.

Respectfully submitted,

VINCENT SO

By



David M. Walters  
Reg. No. 53,904  
Tel.: (613) 232-2486 ext. 240

Date: May 29, 2007

RAB:JFS

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**